Dialog Search For 09/874,717
========
b all
sf all
s (MEASURE OR MEASURING OR MONITOR OR MONITORING OR GATHER OR
    GATHERING OR COLLECT OR COLLECTING)(2W)(USAGE OR UTILIZATION-
)(2W)(DATA OR STATISTICS)
b hits
s (MEASURE OR MEASURING OR MONITOR OR MONITORING OR GATHER OR
    GATHERING OR COLLECT OR COLLECTING)(2W)(USAGE OR UTILIZATION-
)(2W)(DATA OR STATISTICS)
Set   Items   Description
S1   1624   (MEASURE OR MEASURING OR MONITOR OR MONITORING OR GATHER OR
              GATHERING OR COLLECT OR COLLECTING)(2W)(USAGE OR UTILIZATION-
)(2W)(DATA OR STATISTICS)
S2   369   S1 AND PD<20010604
S3   37077 S2 AND (PRINTER OR COMPUTER OR PDA OR PALM OR SERVER)OR(EL-
              ECTRONIC)(2W)(DEVICE)
S4   174   S2 AND (PRINTER OR COMPUTER OR PDA OR PALM OR SERVER OR (E-
              LECTRONIC(2W)DEVICE))
S5   81   S4 AND (APPLICATION OR ((COMPUTER OR SOFTWARE)(1W)(PROGRAM-
              ))(2W)(USAGE OR UTILIZATION))
========

(Reference 1)
2/9/4   (Item 3 from file: 9)
DIALOG(R)File   9:Business & Industry(R)
(c) 2005 The Gale Group. All rts. reserv.
02333443 Supplier Number: 25917584   (THIS IS THE FULLTEXT)
Printer Line Offers 'Net, Remote Management Functionality
(Hewlett-Packard introduced the Color LaserJet 4550 printer line which   features embedded Web server
functionality and improved ease of use and   network manageability)
Graphic Arts Monthly, v 72, n 12, p 70
December 2000
DOCUMENT TYPE: Journal ISSN: 1047-9325 (United States)
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 290
TEXT:
Staff
HP's easy-to-use Color LaserJet 4550 printer line is empowered for use on networks and the Web.
Hewlett-Packard (HP) Company, Palo Alto, Calif., announced in mid-November the availability of its Color LaserJet
4550 printer family, featuring several Internet-enabled technologies and remote management tools. Engineered
improvements
Say company officials, improved ease of use and network manageability are two of the new features found in the
printer line; a third feature is embedded Web server functionality that supports remote management from a
standard Web browser.
 Strong acceptance of these features is anticipated from workgroup environment network managers, claims HP, as
the features will allow users to customize printer alerts as well as monitor and mange usage and consumables
statistics .
Ready for e-services
Model 4550 has been designed to support future e-services solutions with an HP ChaiServer Embedded Virtual
Machine (EVM). This open-architecture programming environment permits users to develop or employ future
custom-built Java applications.
Performance within the 4550 printer family has been improved by way of a 233-MHz processor, the addition of 128
MB of RAM (upgradeable to 192 MB), and a five-GB hard disk. These additions allow the printer to output multiple
original copies at engine speeds, while network bandwidth is improved using an HP JetDirect 610N network card.
Engine speed is four ppm for color and 16 ppm for monochrome print jobs.
The base model 4550 printer, which has a list price of $2,569, features a 400-sheet input capacity, while the top-of-
the-line 4550HDN, which lists for $5,499, features RIP-once technology and the ability to store jobs for demanding
workgroups.
Two additional Color LaserJet models, 4550N and 4550DN, have list prices of $3,029 and $4,819, respectively.
The 4550N provides the same features as the base model plus a 10/100TX card, while the 4550DN has a 500-
sheet input design plus duplex capability.
    Copyright 2000 Reed Elsevier Inc.

(Reference 2)
5/9/2   (Item 2 from file: 9)
DIALOG(R)File   9:Business & Industry(R)
(c) 2005 The Gale Group. All rts. reserv.
00569652 Supplier Number: 23078816   (THIS IS THE FULLTEXT)
Elan Ships Consolidatd Licensing Tool
(Elan Computer Group has introduced SoftWatch for Windows NT software   licensing tool that allows administrators to track software applications   usage from a single server)
CommunicationsWeek, n 532, p 443
November 21, 1994
DOCUMENT TYPE: Journal ISSN: 0748-8121 (United States)
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 236
TEXT:
By TIM WILSON
MOUNTAIN VIEW, CALIF. Elan Computer Group Inc. has taken the wraps off a new software-licensing tool that lets administrators track Microsoft Corp. Windows, Unix and Windows NT application usage from a single server . SoftWatch for Windows NT lets administrators   gather consolidated usage statistics on all of the Windows, Unix and Windows NT applications running on the network, elan said. This information can help administrators plan for software purchases in the future.

In addition, the information ensures that the use of licensed applications stays within legal limits, according to the company, based here.

"The task of monitoring and controlling software application usage over heterogeneous networks is a growing concern for system administrators," according to ken Greer, president of Elan.

"This tool gives systems administrators a single point of control for distributing applications across heterogeneous networks," he added.

Central Server

SoftWatch for Windows NT runs on a central server that has the ability to communicate with Windows and Unix clients via TCP/IP, according to Elan. Under Windows NT, the SoftWatch tool is controlled and monitored from a custom-control-panel application .

On the client end, Windows, Unix and Windows NT applications that use SoftWatch will automatically access the SoftWatch server to request permission to use a particular application . Systems administrators are able to monitor the usage of each SoftWatch-enabled application from the server , according to elan.

The SoftWatch for Windows NT licensing tool is available now. A 25-client package costs $195.

Elan can be reached at 415-964-2200.

SOFTWATCH 34
ELAN

TEXT: David Jordan
The time for usage-based billing is here, but measuring and collecting usage data is not easy. Here are the pros and cons of various approaches.

ISPs are finally figuring out that flat-rate pricing doesn't work for every customer. Today, ISPs are offering access to the Web, to Web-based application services, voice over IP (VoIP), Web hosting, virtual private networks (VPNs), e-commerce services, and video/audio conferencing and broadcasting.

It's time for IP networks to abandon standard flat-rate pricing models in favor of usage-based billing. But given that the Internet functions in a heterogeneous, multivendor IP environment, how can usage data be measured and collected?

Traditionally, telephony providers have collected information from voice switches, generally rendered in Bellcore AMA Format (BAF). These records, collected by the mediation system, are consolidated, formatted and sent to the billing system. The interface is relatively simple: The switch is the meter that creates the accounting records; the mediation system collects information from the switches; and the billing system receives the consolidated records from mediation.

Unfortunately, the IP world is more complex, with a mix of standard and proprietary solutions, creating a confusing array of metering and data collection approaches. IP usage data is collected from a multitude of devices, including routers, switches, gateways, servers and the network itself, and used as the basis for usage billing. The best way to evaluate IP billing options is to weigh critical business factors such as the granularity and accuracy required, and budget constraints that drive cost efficiency, scalability and flexibility. These considerations help determine the optimal choice to support today's business models, network architecture and services infrastructures, and lay the groundwork for future business and usagebased pricing models.

There are five main classifications of data collection technology:

1. Proprietary device-based log files;
2. Standards-based network device interface activity (SNMP MIB-II);
3. Proprietary network activity-based flow meters: (e.g., Cisco NetFlow(TM)-enabled routers and switches);
4. Standards-based network monitoring MIBs: RMON and RMON-II;
5. Proprietary network activity-based session reconstruction.

Log Files Log files are a generic application programming interface (API) that can be used by a device-based accounting process to create persistent records for collection and processing by a mediation system or data warehouse. ASCII log files are created by gateways, firewalls, application and proxy servers and contain types of records such as comma-separated variables (CSVs) and tag-value pairs.

CSVs are useful when the number of fields in the record is fixed and most records contain the same fields. The data collector must know the exact format of the files to be scanned. When the file format or content changes, token and parsing definitions must also be modified.

Tag-value pairs are not position sensitive and are useful when the fields contained in log file records vary. Parsing tag-value pairs relies upon pattern matching, which is more complex and requires more processing than CSVs. The significant benefit of tag-value pair representation is improved flexibility.

For these reasons, log files are not the preferred approach. In certain environments, however, session reconstruction or flow metering is not possible. In these cases, data collection from a log server may be the only practical method available. SNMP MIB-II Dedicated Access

The simple network management protocol (SNMP) management information base (MIB) is an interface between an IP SNMP manager (data collector) and an agent (device/meter). Most IP router and switch vendors support MIB-II. The manager periodically polls the agent for sets of port number indexed MIB-II objects, which include activity counters continuously incremented by the router or switch as packets are sent or received through a particular port. Normalized accounting records require that the collector maintain current and previous counter values. As SNMP responses are received from the routers and switches, the data collector must subtract each previous absolute

integer counter sample from the current figures. The result is called a "delta sample" or differential accounting record, representing aggregated activity for a span of time.

Each SNMP MIB defines a set of objects that are available from the agent for data collection. MIB-II, the most common MIB that is supported by multiple vendors, includes interface status and time of last status change, the number of bytes and packets transmitted for unicast, multicast and broadcast, and the number of errors. MIB-II is useful in dedicated-access, router-based environments where volume per port is required. MIB-II's effectiveness, however, is limited to dedicated-access environments because records are indexed for each port configured in the router or switch. If the association between each port and customer is static, accounting records can be accurately mapped from the access port index number to the customer ID. If access port mapping is dynamic, at least one field of MIB-II data must be mappable to the customer, such as an interface IP address or interface description. In addition, the MIB-II data collector must define and use a key field to reliably associate data samples after a router bas been reconfigured.

MIB-II information can be very useful for the simple burst mode, dedicated-access charging models typical of today's large-scale ISPs. MIB-II's wide implementation provides a very efficient data collection mechanism, and access-port-level error rate and throughput performance, volume and availability.

Proprietary Flow Meters

Proprietary network activity-based flow meters, such as Cisco NetFlow(TM), are based on Layer 3 views of network traffic. IP packets are correlated, analyzed and statistically represented as flows. Flow-based analysis examines each packet's IP header, such as source IP address or port number; destination IP address or port number; number of bytes and packets sent or received; and QoS requested.

NetFlow contains a rich set of IP router-based information because that information exists within the router and is correlated with incoming flows to perform normal routing. NetFlow provides value for:

* IP traffic-routing analysis, such as inter-autonomous system flow, used for router optimization;
* Class-of-service details based on the IP type of service (ToS) bits;
* Flow-level granularity with index numbers that provide direct mapping to dedicated access customer links and network topology;
* Solutions that require aggregations based on router-based information such as IP subnets, source and/or destination autonomous systems.

RMON and Session Reconstruction

Another approach to IP data collection called session reconstruction passively monitors IP network packets and decodes data beyond the IP header. This technique analyzes IP packets at the application layer, creates session and application transaction accounting records, and uses network probes to collect packets in real time. The standard SNMP MIB that defines packet traffic accounting information is called RMON-II

RMON, the initial specification that was limited to link layer packet accounting, and its successor, RMON-II, were designed years ago for fault analysis and network-level performance statistics. The RMON-II MIB specifies nine distinct MIB groups, including packet capture and alarms. Technically, a specification compliant RMON-II implementation must support all nine MIB groups (although many RMON-II agents are embedded in the system) and containt a stripped-down four group RMON implementation that does not provide comprehensive IP accounting information. Further, many RMON-II probes are configured to "rove" over multiple network segments, statistically sampling to detect problems. While useful for troubleshooting, this approach does not work for accurate accounting records, which demand complete data collection coverage. Finally, the RMON-II standard does not specify which, if any, applications a vendor must support. Many support a relatively modest subset of IP applications supported by typical ISPs today. Unlike current RMON-II implementation, the session reconstruction technique has built-in support for many applications that are critical for IP service level management, marketing intelligence and billing mediation. These include Real-time Streaming Protocol (RTSP); H.323 for IP telephony and video conferencing; Hypertext Transfer Protocol (HTTP) for Web traffic; Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP3) for e-mail and messaging services; File Transfer Protocol (FTP); Network News Transport Protocol (NTTP); Remote Authentication Dial-In User Service (RADIUS) (standard-based user authentication and session statistics); and Dynamic Host Configuration Protocol (DHCP) for dynamically assigning IP addresses.

This approach also provides detailed session and application information. Session reconstruction has distinct advantages because it creates normalized performance and accounting records called Internet Protocol Data Records (IPDRs).

The complexity of IP metering and data collection challenges service providers seeking to build usage-based pricing models. The best approach is a tailored solution that offers a suite of metering and collection technologies, including session reconstruction, NetFlow, Log Files and SNMP. Based on a customer's business model, network architecture and objectives, this method delivers an efficient, accurate, flexible and reliable IP data collection solution.

David Jordan is a senior product manager at Narus. (djordan@narus.com)

Pros

* The widest range of service provider application protocols
* Significant coverage due to vendor and platform independence
* Efficient means of collecting application layer data
* No impact on network devices to collect data
* Little impact on network bandwidth to upload summarized session activity
* Variable levels of granularity based on need
Cons
* Inability to handle encrypted traffic * Inability to capture device-specific information
* Expensive coverage for highly meshed, nonhierarchical network architectures
Pros
* Persistency
* Highly accurate data
* Ease of programming, which requires access to a local or networked file system
Cons
* Device overhead is required to create and up date files
* Additional overhead is needed to access files for data collection
* Dependency on file system reliability * File scanning lag-time delay
* Limited scalability
Pros
* Wide coverage across multiple vendors' IP router and switch information
* A single manager/data collector implementation that works for multiple MIB-II agents
Cons
* Aggregate volume over time is very limited--there are no details regarding type of traffic, source and destination, or user-level quality of service (QoS)
* Normalization must be performed by a data collector. If the data collector loses state, for example, the meaning of the current counter value is lost because there is nothing to compare it with to create delta output. The result is lost revenue. Pros
* Router-based data is precorrelated with usage information
* Application layer associations can be made in many, but not all cases
* Most Cisco routers and switches support NetFlow
Cons
* Router performance may degrade with NetFlow enabled
* Dearth of coverage for non-Cisco devices
Data is examined only from an inbound perspective (packets received by a router). Expensive computing is needed to associate bidirectional traffic flows and may not be 100-percent accurate.
* There is no guarantee that all exported flow data has been received and processed by the collector, a significant disadvantage for revenue assurance. * Aggregation heuristics must be applied to "guess" the actual application associated with the flow. This complicated, expensive procedure is about 90 percent to 95-percent accurate in most environments.

ABSTRACT: Companies have monitored employees for security and work measurement purposes for years.
However, the scope of monitoring activities has expanded in recent years with development of electronic tools, and
the number of companies that monitor employee activities has also increased. Given the growth in electronic
monitoring activities, certified public accountants increasingly are expected to respond to their client's questions
with respect to both the tools available to monitor employee activity and the potential legal and social impacts of
using those tools.
TEXT: Companies have monitored employees for security and work measurement purposes for years. However,
the scope of monitoring activities has expanded in recent years with development of electronic tools, and the
number of companies that monitor employee activities has also increased. According to a June 22, 2000 report in
USA Today, about 74 percent of companies currently conduct some form of electronic monitoring of employee
activities whereas in 1977 only 35 percent of companies were engaged in electronic monitoring.1 Given the growth
in electronic monitoring activities, CPAs increasingly are expected to respond to their client's questions with respect
to both the tools available to monitor employee activity and the potential legal and social impacts of using those
tools.

Activities Monitored

At many companies, access to the Internet has replaced the office water cooler as a social gathering place within
the work environment, and managers are concerned about the potential loss of productivity and the security of
proprietary information. Observing idle time around the water cooler is easy, but electronic activities are not so
visible. Likewise, securing the company data was easier when physical removal from the premises was the only
major threat.

Mark F. Asman, Ph.D., CPA, CDP
Patricia Essex, Ph.D., CPA

In the past, most workplace monitoring activities required the presence of a physical monitoring device such as a
video camera or a person. Electronic monitoring of e-mail, computer files, Web sites accessed, keystrokes, phone
time and other computer-related activity does not require a physical presence and can be hidden completely from
the monitored employee. The diversity of electronic monitoring of employees is captured in the following table from
data gathered by the American Management Association's 2000 Monitoring and Surveillance Survey.

Monitoring Tools

Electronic monitoring tools fall into one of two categories: (1) those that monitor all employee computing activities or
(2) those that monitor only Internet-related employee activities. Within the second category, tools are available that
can monitor all Internet-related activities or only selected tasks such as e-mail. E-mail appears to be of particular
interest to many organizations. Sales of e-mail monitoring tools are expected to reach $70 million this year and to
double within the next few years.3

An example of software that monitors all computing activities is Investigator by WinWhatWhere Corporation. The
program, installed on each user's computer, can log every Web site visited, documents and files opened, and time
spent on each application. Because Investigator captures all keystrokes, it also can monitor deleted or unsent e-
mail messages and documents. Investigator's installation is not apparent to the user. Prices start at $99 per user
with downward adjustments based on volume.

An example of software that moni- tors only Internet usage is NetSpective by Telemate.Net Software, Inc. This
program is installed on an organization's proxy server or firewall and monitors all employee Internet activities,
including e-mail, Web site visits and downloads. NetSpective can block access to nonproductive Web sites or to
high band-width downloads (such as audio or video files). The program can report on Internet e-mail traffic and

band-width consumption by users, groups, or peak times. The software's drill-down reporting capability permits network managers to monitor virtually any usage down to the user level. Prices for NetSpective start at $995 per proxy server for simple Internet usage reporting and can range upward to $15,000 per proxy server if a business wishes to implement all features of the system including active blocking of access to specific Web sites or other Internet activities.

Diversity of Monitoring Activities2

Legal Issues

Government versus Private Employee Rights

CPAs who have government agencies as clients should be aware of the fact that monitoring of employees in such agencies normally is prohibited by the Fourth Amendment to the US. Constitution, which bars unreasonable searches and seizures. In addition, several states have specific constitutional provisions that recognize state employees' rights to privacy.4

Unlike public employees, private employees are not afforded a constitutional right to privacy in the workplace. In general, if employees are informed of the surveillance possibility, and the activity is not prohibited specifically by contract or law, surveillance is permitted.5 Sometimes, employers have won court decisions in their favor when sued for monitoring activities even ofter providing assurances of privacy.6

Current Litigation and Proposed Legislation

Some employees have brought civil damage suits against their employers under the Electronic Communications Privacy Act (ECPA) of 1986. With respect to electronic communications, this act prohibits unauthorized interception and unauthorized retrieval from storage media, such as hard disks. The act provides an exception for employers; specifically, if one of the parties to the communication has consented, interception is allowed. Whether the ECPA applies to communications over a business' private network is unclear at present, even more so when a business' private network utilizes an external network such as the Internet.7

Legislation currently before the Congress will, if adopted, prohibit companies from secretly monitoring their employees' e-mail and Internet usage. A bill before the House, known as the Notice of Electronic Monitoring Act, would not prohibit employee monitoring but would (1) require notification to employees of the firms monitoring practices on an annual basis or whenever policies are changed, (2) require specific disclosure as to the frequency of monitoring, where the information is stored and how it will be used, and (3) limit civil damages to $20,000. Essentially identical legislation is pending in the Senate.8 Similar legislation has been proposed in prior congressional sessions, and it seems likely that some legislation will be passed in the relatively near future.

International Legal Ramifications

Since many clients have international operations that utilize Internetbased systems, CPAs should be aware that other countries such as Canada and England have different legal frameworks covering electronic monitoring of employees. A measure taking effect in October 2000 in England makes it illegal to monitor employees electronically without consent-even for purposes such as staff training, marketing and market research.9 The Criminal Code of Canada prohibits the interception of private communications in that country.10

In general, employers can protect their legal right to monitor employee e-mail and other Internet-related activities by properly notifying employees of their monitoring policies and obtaining employee consent. The American Management Association recommends the following to its member companies:

Policies and practices in electronic monitoring and surveillance should be promulgated and posted so that employees are aware that their actions and communications are subject to recording and review.11

In its 2000 survey, the American Management Association found that over 85 percent of reporting firms inform employees of their electronic monitoring policies."

Monitoring and Employee Morale Issues

Beyond the legal issues, CPAs and their clients must be cognizant of the possible impact of electronic monitoring on employee trust and morale. Because broad-based monitoring of key strokes or Internet-related activities is a relatively recent phenomenon, little specific empirical work centered on such practices exists. However, electronic monitoring of employee activities in call-centers has been widely studied and provides some pertinent insights.

Privacy advocates have written extensively on the negative aspects of employee monitoring. However, empirical research examining call-centers does not seem to support the hypothesis that employee monitoring necessarily generates negative employee responses. A comparison of employee attitudes in five different companies in five different industries suggests that whether employees respond positively or negatively to monitoring depends on how the monitoring is implemented and how the collected data is used.13

Whether monitoring is for purposes of reviewing employee performance, protecting company secrets, or enforcing workplace rules, research results suggest that employees will be more satisfied if they believe that the system is procedurally fair. A process is considered procedurally fair when it includes input from all affected parties, is applied consistently, suppresses bias, is as accurate as possible, provides a mechanism for correcting errors and is ethical.14 Perceived lack of procedural fairness in electronic monitoring can lead to undesirable negative employee reactions such as withdrawal, sabotage, resignation or some other form of diminished organizational citizenship.15

An electronic employee-monitoring system is more likely to find acceptance with employees if, in addition to being procedurally just, the use of the collected data is thought to be distributively just. A system is considered distributively just if employees perceive the outputs of the system as related fairly to personal outcomes, such as individual pay or promotion. Thus, if employees perceive that pay or other rewards are distributed in a way that is consistent with the data reported by the monitoring system, the system will be thought of as distributively just. Perceived lack of distributive justice in an electronic monitoring system has been shown to be associated with lower job satisfaction in non-government organizations.16

Recommendations

To Monitor or Not

Unless the employer is a government agency, a fundamental right to monitor employee activity exists at the present time. As clients seek advice on the implementation of employee monitoring tools, the first question that must be addressed is the business purpose of the monitoring. Electronic monitoring is costly, and the benefits should exceed the costs. In addition to the software costs cited earlier, additional costs include the time to review and use the collected data and the high cost of employee dissatisfaction if the electronic monitoring system is not properly designed and implemented.

Proponents of monitoring argue that the economic benefits include reduction of nonproductive use of company assets and the safety of proprietary information. Unfortunately, clever employees who wish to steal proprietary information are often knowledgeable enough to elude any monitoring system in place. Further, if the productivity of an employee meets or exceeds the expectations of the employer, little reason to monitor his or her activities exists. In fact, opponents to monitoring argue that a productive employee's personal use of the firm's electronic applications is a good employer accommodation that allows such employees to be the productive people that they are. Monitoring opponents also maintain that employees performing at substandard levels are unlikely to change just because a monitoring system is put into place.

Compliance with legal requirements is another reason to implement electronic monitoring. In regulated industries, taping telemarketing activities may provide both the company and its customers some degree of legal protection by providing accurate records of activities. Electronic recording and storage of activities might be considered part of the company's due diligence in keeping adequate records and files of its activities.

Arguments are sometimes made that electronic monitoring is one way that an organization can guard against an employee's unwitting exposure to offensive graphic material on a colleague's computer screen or one employee harassing another through email or other electronic communication. Employers do not have a duty to discover harassment. They do have a clear duty to take action to prevent the recurrence of such activity once discovered. However, that would involve monitoring a specific individual's activities rather than an entire work-force, clearly a much less costly proposition.18

Implementation Guidelines

If a client is convinced that sound business reasons exist to implement electronic monitoring, then CPAs must be prepared to offer sound implementation advice. The following guidelines appear to provide a reasonable basis for monitoring activities in order to avoid potential problems.

* Establish a reasonable and clear policy with respect to Internet activities. A general policy stating that illegal and non-work-related tasks done over the Internet are prohibited should be sufficient. Policies that attempt to list every non-permitted activity typically fail because of overlooked or new activities. Further, detailed policies create the illusion of acceptance for any activity excluded from the list.

* Create a privacy policy that clearly informs employees about the monitoring activities that are in place and the use of the gathered data. Then, follow the stated policy. Changes in either monitoring efforts or usage of gathered data should be announced publicly prior to implementation. Care should be taken when developing privacy policies so that employees understand the fairness of both the policy and the use of gathered data. Stated policies that are consistently followed are the best defense against employee lawsuits. Provide security training for everyone with access to the Internet. Employees need to be aware of the potential harm that can occur-either to themselves as individuals or to the organization-given the insecure nature of Internet transactions. Employees must realize that privacy and security of e-mail, Web sessions and other Internet-based activities do not exist and that any information passed between computers during such sessions is open to others both inside and outside the firm.

Conclusion

While electronic monitoring of employee activity is widespread and growing, empirical work that provides insight into the costs and benefits of such monitoring is not yet available. Results of monitoring activity can be neutral, positive or negative to an organization's productivity and employee morale depending on implementation.

Managers must explore the costs and benefits of electronic employee monitoring technology to see if the benefits exceed the costs. When a decision is made to implement tools that electronically monitor employee activities, managers should develop policies for implementation that are procedurally and distributively just and emphasize performance rather than control. Without adequate supporting policies, achieving the expected benefits may be difficult.

Endnotes

1. USA Today, June 22, 2000, p. 131.

2. Greenberg, Eric Rolfe, Carol Canzoneri, and Joe Annamma, "A 2000 Survey, Workplace Testing; Monitoring and Surveillance," American Management Association, p. 1.

3. Informationweek, February 21, 1000, pp. 142-146.

4. Overly, Michael R., E-Policy, American Management Association, 1999, pp. 23-30.

5. Hertenstein, Edward, Dispute Resolution Journal, Vol. 52, No. 4, Fall, 1997, pp. 36-44. 6. See the California case of Shoard v. Epson America, Inc.

7. Overly, Michael R., Ibid.

8. Thibodeau, Patrick, Computerworld, September 11, 2000, pp. 1; 95.

9. Eaglesham, Jean, Financial Times, London Edition, August 3, 2000.

10. Gahtan, Alan, Canadian Business and Current Affairs, March 1997, p. 2.

11. Greenberg, et. al. Ibid. 12. Ibid.

13. George, Joey F., " Computer -Based Monitoring: Common Perceptions and Empirical Results," MIS Quarterly, December 1966.

14, Leventhal, G.S., "What Should be Done with Equity Theory? New Approaches to the Study of Fairness in Social Relationships." In K. Gergen, M. Greenberg, & R. Willis (Eds.), Social Exchange: Advances in Theory and Research, pp. 27-55. New York: Plenum, 1980.

15. Kidwell, Jr., Roland E. and Nathan Bennett, "Employee Reactions to Electronic Control Systems, The Role of Procedural Fairness," Group & Organizational Management, Vol. 19, No. 2, June 1994, pp. 203-218. 16. Ibid.

17. Hodson, Thomas J., Fred Englander, and Valerie Englander, "Ethical, Legal, and Economic Aspects of Employee Monitoring of Employee Electronic Mail," Journal of Business Ethics, Vol. 19, No. 1, March 1999.

Mark F. Asman, Ph.D., CPA, CDP, Ernst & Young, is professor emeritus of accounting and MIS at Bowling Green State University in Bowling Green, Ohio 43403.

Patricia A. Essex, Ph.D., CPA, is an associate professor of accounting and MIS at Bowling Green State University in Bowling Green, Ohio 43403.

The authors can he reached at masman@cba.bgsu.edu or pessex@cba.bhsu.edu of or by telephone at 419.372.277.

ABSTRACT:
A new class of tools offers Internet service providers (ISPs) a means to charge customers for regular, premium, and high-test Internet services. At least 12 vendors are selling billing systems that can capture information about IP usage from different network devices and then parse it to produce invoices for millions of subscribers. To see how these systems stack up, it is important to begin with the basics. One basic question is what hardware and software do these systems actually poll straight from the box. Routers, directories, switches, and probes are all a possibility. It is also important to check if the vendor has cut any deals with third-party applications vendors that can dice and slice usage data from even more sources and deliver it in a neat little bundle. With regards to the invoices, selective and rate-based billing are the rule, but not all systems post charges to the Web in real time. It is also critical to obtain the big picture on price, and to ask for and obtain detailed estimates up front. When it is all summed, IP billing systems can cost millions of dollars. As such, certain billing vendors are offering outsourced services. However, for many carriers and ISPs, the investment is worth it. According to Jack Bowers, CIO of Internet products and services at Bellsouth Corp. (Atlanta, GA), they are doubling and tripling their subscriber base and confronting small, nimble competitors. Bowers is supervising the installation and customization of a package from Portal Software Inc. (Cupertino, CA), which he hopes will be producing bills by the end of summer 1999. Article discusses some of the excellent sources of utilization data, such as network probes and monitors.
TEXT:
A new class of tools gives ISPs a way to charge customers for regular, premium, and high-test Internet services
By Mary Jander
BACK WHEN AL GORE was allegedly building the infohighway, road rage wasn't a worry. Maybe he should try phoning a few ISPs next time he's looking for campaign contributions; they can fill him in on the problem. Their corporate customers are demanding high-octane offerings like e-commerce and VOIP. Meanwhile, they don't have a way to bill for premium services; pretty much all they can do is charge a flat toll at their Internet onramps. Talk about running on empty...

Don't strip the gears; help is on the way. At least a dozen vendors are selling billing systems that can grab information about IP usage from various network devices and then parse it to generate invoices for millions of subscribers. Feeling better? Then get down to the real work of seeing how these systems stack up--with a little help from DATA COMMUNICATIONS.

Start with the basics. What hardware and software do these systems actually poll straight from the box? Switches, routers, probes, and directories are all a possibility. Check to see if the vendor has cut any deals with third-party application vendors that can dice and slice usage data from even more sources and deliver it in a neat little bundle. How much customization is needed to get the package to tackle the tasks at hand, and does the vendor sell development kits, APIs, or even expert help to ease the effort and extend a product's reach? Then give those invoices a good going-over: selective and rate-based billing are the rule, but not all systems post charges to the Web in real time. And be sure to get the big picture on price. Will the system run on the current infrastructure or are new hardware and software needed? Ask for--and get--detailed estimates up front. Base prices may not buy much, and specific features are often priced separately. (Again, customization can be a killer.) When it's all tallied, IP billing systems can cost millions of dollars. That explains why some billing vendors are offering outsourced services.

For many carriers and ISPs, though, the investment is worth it. "We're doubling and tripling our subscriber base and facing small, nimble competitors," says Jack Bowers, chief information officer of Internet products and services at Bellsouth Corp. (Atlanta). "We need to get services out quickly and successfully." Bowers is overseeing the installation and customization of a package from portal Software Inc. (Cupertino, Calif.), which he hopes will be generating bills by the end of this summer. While he won't say what he's spent, he's "certain that return on investment will take care of itself" once the system is up and running.

IRONIC INTERLUDE

Call it an Internet irony. ISPs are rolling out tomorrow's IP services, but they're stuck with yesterday's billing technologies. That means they're limited to charging flat-rate tariffs for Internet access. And without a way to charge a premium for premium services, ISPs can't get the income they need to upgrade and extend their networks. That means they can't compete with rivals, and customers don't get the services they want.

Ironically, finding the right billing system can be more of a challenge than upgrading the network itself. Adding bandwidth or server capacity follows established procedures. Billing calls for new technology.

Why? Because conventional telco billing systems are designed to work with voice networks. Creating a bill means obtaining a log file of CDBs (call detail records) maintained in a Bellcore standard format on voice switches. The billing system reformats this data for use in invoices.

Why not do the same for IP? For starters, voice calls are circuit switched; IP is a connectionless, packet-oriented protocol. That makes it tougher to track traffic. And telco billing systems only have to deal with one type of service; ISPs want to charge different rates for a range of different apps.

Then there's the lack of standards. There is no analogue for voice CDRs in IP, which means billing packages can't request usage data from network switches and be certain they'll always get it in the same format. That's a huge problem, since Internet data is typically handled by several providers' networks. Without some uniform way to track traffic, there's no way for ISPs to exchange billing data or charge for carrying competitors' traffic. They can only charge customers a flat-rate admission fee at network entry points. While efforts are underway to standardize IP billing records, it's still early days (see "Triple A Standards").

THE BILLING BEAT

It's a formidable set of challenges, but some 12 vendors say they're up to the task (see Table 1). These include suppliers of traditional telco billing systems that have recently made the move to IP, like Amdocs Ltd. (St. Louis), Belle Systems A/S (Holbaek, Denmark), Cabledata Inc. (Rancho Cordova, Calif.), Daleen Technologies Inc. (Boca Raton, Fla.), Geneva Technology Ltd. (Cambridge, U.K.), Kenan Systems Corp. (Cambridge, Mass.), Portal, Saville PLC (Burlington, Mass.), Solect Technology Group (Toronto), and Teleknowledge Ltd. (Kfar Saba, Israel). There also are newcomers like Apogee Networks Inc. (Rochelle Park, N.J.) and Tribeca Software Inc. (New York).

Since there are no IP CDRs, all these vendors cobble together usage data from a variety of sources, including RMON (remote monitoring) probes, Radius (remote authentication dial-in user service) servers, and router software agents. The gathered information is pulled into a database, where it's sorted, analyzed, and matched with pricing variables.

With so many sources of information available, where a billing system gets its data is an issue. For instance, since Radius servers track who accessed a particular Web host and for how long, their log files can be valuable for billing--especially when tallying up charges for Web- server space. Apogee and Belle furnish direct links to Radius servers. Belle actually goes one better, bundling an integral Radius server in its IMS; this setup lets ISPs add authentication to offerings without customization.

But Radius servers only disclose a portion of the picture; they can track access to Web servers but can't report on network utilization--how much bandwidth on a given IP connection was consumed by a particular app or end-user. This sort of info is becoming increasingly important to providers as they start selling multiple IP services--e-mail, VPNs (virtual private networks), and so on--to multiple customers over one high-speed link. PROBING QUESTIONS

Network probes and monitors are another excellent source of utilization data. Apogee's Netcountant NSP and Tribeca's NetCFO, for example, can retrieve RMON 2 data from these devices. Routers and switches from Cisco Systems Inc. (San Jose, Calif.) are also a good source. These products run Netflow, a proprietary flow-monitoring utility that keeps tabs on packet activity. Most billing vendors can tap directly into Netflow data; the exceptions are Amdocs, Cabledata, Saville, and Teleknowledge.

Combining Netflow data with information from Radius servers, RMON probes, and other sources lets ISPs charge customers for the specific IP bandwidth they use, rather than hitting them with a one-size-fits-all invoice. For example, a group of users identified by a Radius server could be billed for the time they're actually logged into an accounting app on the intranet server . What's more, their application flow could be traced through the Cisco router and matched up to session logs.

Apogee has devised a savvy scheme that translates Netflow and RMON/RMON 2 data into a common format that's fed to an object-oriented database maintained by Netcountant. Carriers can run queries against the database using a graphical interface. The vendor says that its approach lets carriers and ISPs quickly view accurate usage profiles and assemble invoices to fit specific services and customers.

Belle Systems' IMS pulls IP usage data from Cisco's 6510 Service Selection Gateway, a device that works with Radius servers to deliver browser-based access to different IP services, such as corporate e-mail or an accounting app. End-users typically reach these services via icons on their desktop. Belle's IMS tracks the Radius server , ensuring that users are billed accurately for IP services used on one network--or even over one connection.

LIFE AFTER CISCO

Cisco isn't the only vendor that billing system suppliers are paying attention to. Cabledata and Solect both tap into the Telcordia Accounting Gateway from Telcordia Technologies Inc. (formerly Bellcore, Morristown, N.J.), a software package that pulls usage information from VOIP (voice over IP) switches.

Apogee recently announced that its billing system can access the Content Smart Web Switch from Arrowpoint Communications Inc. (Westford, Mass.), a load-balancing Web server . This enables the Netcountant to gather usage data based on Web addresses, a useful tool for providers of managed application services and Web storefronts who need to know how much bandwidth and system resources are consumed by customers accessing the same servers over the same connections.

Apogee also has built an interface to the Appswitch 2000, a Layer 7 switch from Top Layer Networks Inc. (Westborough, Mass.) that makes decisions based on application -layer information. This could come in handy for managed application providers who need to track activity on their servers for multiple customers (see "Hosting Services: Now Accepting Applications," March 21, 1999; www.data.com/issue/ 990321/hosting.html).

ROLL YOUR OWN

Rather than trying to offer off-the-shelf interfaces to an ever-growing list of data sources, many IP billing vendors sell development kits or APIs (application program interfaces) so carriers and ISPs can create their own hooks. A carrier could, for example, use an API to write software that imports a log file of usage data from a high-end data switch. Or a special interface could be set up in order to monitor usage on Web or e-mail servers. Sounds pretty slick, but ISPs will only benefit from these tools if they have the in-house expertise to program them. What's more, these utilities don't come cheap. Solect, for instance, charges $50,000 for its development kit. Ultimately, ISPs and carriers need to weigh the cost of using APIs against the customization charges exacted by vendors.

Further, not all vendors offer APIs. Apogee believes doing so would undercut its goal of selling shrink-wrapped systems. "If our goal is to give carriers off-the-shelf billing, why would we offer them APIs?" says Pablo Tapia, president and chief executive officer.

But even APIs or extensive customization may not be enough. Just because a billing system can pull usage data from routers, probes, and the popcorn machine in the corporate lunchroom doesn't mean it can make sense of its findings. Converting the input from external data sources into accurate invoices is no easy matter. To ease the effort--and extend the reach of their systems--some vendors are forging technology alliances with third parties that build so-called data collectors, software that specializes in pulling and parsing IP information. These include Hewlett-Packard Co. (HP, Palo Alto, Calif.) as well as startups Narus Inc. (Redwood City, Calif.) and Xacct Technologies Inc. (Santa Clara, Calif.). Xacct's Xacctusage, for example, obtains IP usage data from routers, switches, hubs, Radius servers, RMON probes, Web and application servers, network directories, databases, and other hardware and software. Once it has what it needs, it slices and dices the data in different ways to get the skinny on IP usage. Xacct usage can compare user logs from Radius servers with the amount of time specific ports on routers were actually open, to pinpoint the use of specific apps and services. It also converts this information into the format needed by a particular billing system. HP's SIU (Smart Internet Usage) and Narus's Intelligence do much the same thing.

Xacct is by far the most commonly used data collector. Billing systems from Amdocs, Cabledata, Daleen, Kenan, Portal, Saville, and Solect all work with it. Belle, Kenan, Portal, and Saville also play with HP's SIU, and Amdocs and Portal also can interface with Narus Intelligence.

THE BILL, PLEASE

Pulling together IP usage stats is only the beginning of the billing process. Invoices still have to be generated. Each of these packages can handle so-called selective and rate-based billing. Selective (a.k.a. hierarchical) schemes let ISPs bill back to specific sites, departments, and individuals. One corporate account, for example, might have a VPN billable to the IT department at headquarters, Internet access billed on a per-site basis, and Web hosting billed to individual divisions and departments.

Rate-based billing, as the name suggests, makes it possible to charge different rates for different IP services--on a single invoice. Rates also can differ within a single service. Thus, guaranteed Internet access would cost more than best-attempt service. As long as a billing system can tap into the requisite sources of usage data, it should be able to deliver rate-based billing without much customization.

Actually, the tricky part for billing vendors is being able to offer information in real time to different ISPs and carriers. The Web can be a huge help here: Amdocs, Belle, Portal, and Solect offer online billing data. But a Web interface is no guarantee that data will be fresh: Apogee and others offer Web postings in near real time, which typically means the information is updated several times a day.

BILLING'S BOTTOM LINE ISPs who think IP billing systems are an idea whose time has come should take a deep breath; these products don't come cheap. Getting a fix on overall costs can be tough, though, since these depend on several factors: how well the system fits with a carrier's current infrastructure; how much the basic software costs (and what it includes); and how much customization will be needed.

Roughly half the systems on the market run under Windows NT: Apogee, Belle, Kenan, Saville, and Tribeca Software. NT servers cost roughly $4,000, and at least one will have to be dedicated to the billing system. The remaining products run on Unix; platforms cost about $10,000 per machine.

Basic prices also vary widely and wildly. Apogee's barebones Netcountant retails for $90,000. That buys a simple billing system that comes with hooks to RMON and Netflow.

Amdocs, in contrast, says most projects start at $10 million. Before they succumb to sticker shock, ISPs should realize that Amdocs and other high-priced vendors specialize in creating custom billing systems for CLECs (competitive local-exchange carriers) and large carriers. And billing is just the beginning. Its systems typically include a full suite of customer care apps, including sales analysis, order entry, and data warehousing. The base price often includes some customization. In fact, professional services may be key to making the product work. "We've got a standard package that we implement quickly with a small number of interfaces for under $2 million," says Richard Aroian, vice president of marketing and strategic alliances at Saville. If this is the bargain price, carriers can bet they'll be paying far more for a range of interfaces and apps.

Belle and Solect, in fact, see their ability to customize their products as a key selling point. "We win deals based on our intellectual property," says Mark Fowlie, director of product management at Solect.

Ultimately, ISPs and carriers need to find the right mix of customization and off-the-shelf functionality. "We started by hiring a consultant, then we chose our own billing product and used its development tools to do much of the integration work ourselves," says Jim Kruger, product manager at Palm Computing Inc. (Santa Clara, Calif.). Palm makes a PDA (personal digital assistant) and offers customers wireless Internet access from Bellsouth. Palm charges customers by the kilobyte; it chose Portal's Infranet and then tweaked it to monitor IP usage. "We saved money over the long run by doing much of the work ourselves," Kruger comments. "And it gave us control over the system that we otherwise wouldn't have had." MARY JANDER is associate managing editor/special projects for Data Comm. Her e-mail address is mjander@data.com.

Table 1: Selected Vendors of IP Billing Software Sources of IP usage data

RMON/ Vendor	Product	Radius	RMON2
Amdocs Ltd. St. Louis, 314-821-3242 www.amdocs.com	Ensemble Circle No. 710	No	No
Apogee Networks Inc. Rochelle Park, N.J., 201-368-8800 www.apogeenet.com	Netcountant NSP Circle No. 711	Yes	Yes
Belle Systems A/S Holback, Denmark, 45-59-44-25-00 www.bellesystems.com	IMS Circle No. 712	Yes	No
Cabledata Inc. Rancho Cordova, Calif., 916-636-5820 www.cabledata.com	Intellicable Circle No. 713	No	No
Daleen Technologies Inc. Boca Raton, Fla., 561-997-1612 www.daleen.com	Billplex Circle No. 714	No	No
Geneva Technology Ltd. Cambridge, U.K., 44-1-223-236-023 www.gtl.com	Geneva Circle No. 715	No	No
Kenan Systems Corp. Cambridge, Mass., 617-225-2200 www.kenan.com	Arbor/Internet Circle No. 716	No	No
Portal Software Inc. Cupertino, Calif., 408-343-4400 www.portal.com	Infranet Circle No. 717	No	No
Saville PLC Burlington, Mass., 781-270-6500 www.savillesys.com	Convergent Billing Platform Circle No. 718	No	No
Solect Technology Group Toronto, 416-363-7844 www.solect.com	IAF Horizon Circle No. 719	No	No

Vendor	Product		
Teleknowledge Ltd. Kfar Saba, Israel, 972-9-7614000 www.teleknowledge.com	B3 Circle No. 720	No	No
Tribeca Software Inc. New York, 212-219-4488 www.tribecasoftware.com	NetCFO Circle No. 721	No	Yes

Vendor	Third-party	Third-party Vendor	
Amdocs Ltd. St. Louis, 314-821-3242 www.amdocs.com	None	Narus Intelligence, Xacct Xacctusage	
Apogee Networks Inc. Rochelle Park, N.J., 201-368-8800 www.apogeenet.com	Cisco (via Netflow), Arrowpoint, Top Layer	None	
Belle Systems A/S Holback, Denmark, 45-59-44-25-00 www.bellesystems.com	Cisco (via Netflow) and Cisco 6510 Service Selection Gateway	HP SIU	
Cabledata Inc. Rancho Cordova, Calif., 916-636-5820 www.cabledata.com	Telcordia Accounting Gateway for VOIP switches (3Q99)	Narus Intelligence, Xacct Xacctusage	
Daleen Technologies Inc. Boca Raton, Fla., 561-997-1612 www.daleen.com	None	Narus Intelligence, Xacct Xacctusage	
Geneva Technology Ltd. Cambridge, U.K., 44-1-223-236-023 www.gtl.com	None	Narus Intelligence, Xacct Xacctusage	
Kenan Systems Corp. Cambridge, Mass., 617-225-2200 www.kenan.com	Cisco (via Netflow)	None	
Portal Software Inc. Cupertino, Calif., 408-343-4400 www.portal.com	Cisco (via Netflow)	HP SIU, Narus Intelligence, Xacct Xacctusage	
Saville PLC Burlington, Mass., 781-270-6500 www.savillesys.com	None	HP SIU, Narus Intelligence, Xacct Xacctusage	
Solect Technology Group Toronto, 416-363-7844 www.solect.com	Cisco (via Netflow), Telcordia Accounting switches	Narus Intelligence, Xacct Xacctusage	Gateway for VOIP
Teleknowledge Ltd. Kfar Saba, Israel, 972-9-7614000 www.teleknowledge.com	None	None	
Tribeca Software Inc. New York, 212-219-4488 www.tribecasoftware.com	Cisco (via Netflow)	None	

Vendor	Online tallies for prepaid customers	System requirements Database	
Amdocs Ltd. St. Louis, 314-821-3242 www.amdocs.com	Yes	Unix, Windows NT, IBM mainframe	
Apogee Networks Inc. Rochelle Park, N.J.,	No	Unix, Object-store Windows NT	

Vendor		OS	Database
201-368-8800 www.apogeenet.com			
Belle Systems A/S Holback, Denmark, 45-59-44-25-00 www.bellesystems.com	Yes	Unix	Oracle
Cabledata Inc. Rancho Cordova, Calif., 916-636-5820 www.cabledata.com	No	Unix	Oracle
Daleen Technologies Inc. Boca Raton, Fla., 561-997-1612 www.daleen.com	Yes	Unix, Windows NT	Oracle
Geneva Technology Ltd. Cambridge, U.K., 44-1-223-236-023 www.gtl.com	Yes	Unix, Windows NT	Oracle
Kenan Systems Corp. Cambridge, Mass., 617-225-2200 www.kenan.com	No	Unix, Windows NT	Any
Portal Software Inc. Cupertino, Calif., 408-343-4400 www.portal.com	Yes	Unix	Oracle, SQL Server
Saville PLC Burlington, Mass., 781-270-6500 www.savillesys.com	No	Unix, Windows NT	Oracle
Solect Technology Group Toronto, 416-363-7844 www.solect.com	Yes	Unix	Oracle
Teleknowledge Ltd. Kfar Saba, Israel, 972-9-7614000 www.teleknowledge.com	No	Unix, Windows NT	Oracle
Tribeca Software Inc. New York, 212-219-4488 www.tribecasoftware.com	Yes	Unix, Windows NT	Oracle

Vendor	APIs sold with package	Price
Amdocs Ltd. St. Louis, 314-821-3242 www.amdocs.com	No	$10 million to $20 million
Apogee Networks Inc. Rochelle Park, N.J., 201-368-8800 www.apogeenet.com	No	$90,000 to $500,000
Belle Systems A/S Holback, Denmark, 45-59-44-25-00 www.bellesystems.com	Yes	Starts at $100,000
Cabledata Inc. Rancho Cordova, Calif., 916-636-5820 www.cabledata.com	Yes	Starts at $100,000
Daleen Technologies Inc. Boca Raton, Fla.,	Yes	$500,000 to $2 million

561-997-1612
www.daleen.com

Geneva Technology Ltd. Cambridge, U.K., 44-1-223-236-023 www.gtl.com	Yes	$500,000 to $2 million
Kenan Systems Corp. Cambridge, Mass., 617-225-2200 www.kenan.com	Yes	Starts at $100,000 (includes $50,000 for software)
Portal Software Inc. Cupertino, Calif., 408-343-4400 www.portal.com	Yes	Starts at $200,000
Saville PLC Burlington, Mass., 781-270-6500 www.savillesys.com	Yes	Starts at $100,000
Solect Technology Group Toronto, 416-363-7844 www.solect.com	No	Starts at $800,000
Teleknowledge Ltd. Kfar Saba, Israel, 972-9-7614000 www.teleknowledge.com	No	Starts at $300,000
Tribeca Software Inc. New York, 212-219-4488 www.tribecasoftware.com	Yes	Starts at $65,000

API = Application program interface
Radius = Remote authentication dial-in user service
RMON = Remote monitoring
SIU = Smart Internet Usage
Triple A Standards

CAN IP BILLING METRICS BE STANDARDIZED? The authentication, authorization, and accounting (AAA) working group of the IETF (Internet Engineering Task Force) is hoping to come up with a standard way to take IP usage data from carrier networks and format it for IP billing systems. But actual specs are a ways off. The group first has to define an underlying architecture. At press time it was on schedule to publish drafts outlining the security requirements and data collection schemes for usage-based accounting. Next, the AAA plans to define how current protocols can be extended to meet these needs. New protocols also will be defined.

The so-called Triple A architecture won't be limited to billing. The group also intends to specify how policy management and authorization functions can be integrated into one management system. It's supposed to wrap up its work this fall. The full agenda can be viewed at www.ietf.org/html.charters/aaacharter.html.--MJ.

Need a vendor-free view on IP billing? Work the Web, starting with these sites:

* http://search.ietf.org/internetdrafts/draft-aboba-acct-00.txt .

The IETF has been into IP billing for years. This draft describes the requirements for a system that monitors performance and maintains usage accounts.

* http://www.tmforum.org/pages/Teams/team1.html

Check out the charter and basic roster of carriers involved in studying billing issues for the Telemanagement Forum, a nonprofit group of international service providers.

* http://www.cni.org/docs/ima.ip-workshop/Sirbu.html

Grad students in the Information Networking program at Carnegie Mellon University offer some smart thinking about security and collecting online payment for IP services.

(Reference 6)

02142368 69798491
Racing to next gen
Young, Deborah
COMPANY NAMES:
Alltel Corp (DUNS:00-790-2802 TICKER:AT SIC:4813 NAICS:513322)
SmarTone Telecommunications Holdings Ltd (NAICS:551112)
Ace-Comm Corp (TICKER:ACEC NAICS:513340)
GEOGRAPHIC NAMES: United States; US
DESCRIPTORS: Wireless carriers; Technological change; Information   management; Internet telephony;
Technological planning
CLASSIFICATION CODES: 9190 (CN=United States); 8330 (CN=Broadcasting &   telecommunications); 5220
(CN=Information technology management)
PRINT MEDIA ID: 36163

ABSTRACT: Carriers often add usage-record generation and collection functions to their systems as an
afterthought. One big lesson Alltel learned from its CDPD experience is that keeping track of IP-services usage
depends on the ability to manage and assign IP numbers and use them as subscriber identifiers. To prepare for the
applications of tomorrow, Alltel is trying to create a billing enterprise that is adaptable and operates on open
architectures. Vendors can help carriers by creating standards-based rather than proprietary architectures for their
products and by considering carriers' billing and back-office needs. Unfortunately, there is more than one answer to
the question of how to collect usage information from IP networks. During the build-out of next-generation networks,
companies will have nationwide networks that will be a mixture of 1G, 2G, 2.5G and 3G technologies. This situation
creates the requirement for convergence at the mediation and/or billing area.

TEXT: The contest ain't over 'til you get paid.

After Maurice Greene sprinted across the finish line ahead of his peers this past summer and won the Olympics
100-meter track and field finals, he had the luxury of putting the race behind him. He could sit back and collect his
gold and glory. Competitors in the race to the next generation have no such luxury. Even if you win the race and the
glory of being the first to launch the newest generation of wireless services in your market, it's a Pyrrhic victory if
you can't monitor, analyze and bill subscribers for the value-added services.

"The focus, like in all new technology, seems to be the technology and the application ," said Martin Demers,
Ace*Comm senior vice president of marketing and development. "Sometimes people forget that somebody has to
pay for all of this. People forget to think about how usage is going to be measured, how usage records are going to
be collected and what (system) they are going to use to do their billing."

Ace*Comm sells mediation and operation-support-- system products that are used to collect call and transaction
data from various sources, including circuit-switched, packet-switched and IP networks. The company works with
vendors such as Cisco Systems, Motorola, Oracle and Siemens to develop products that can be integrated into
switching and software systems. (See Figure 1 on nage 32.)

While working with network and switch vendors, Demers has observed that carriers often add usage-record
generation and collection functions to their systems as an afterthought. They focus first on the technology, Demers
said, then figure, "Somebody needs to pay for this. We better generate usage records."

Figure 1.

Lessons From the Past

What are carriers doing to prepare their networks to collect data from IP networks?

"Lighting a lot of candles, I would assume," Steve Lyons joked.

Lyons, Alltel senior business analyst for billing, then explained why Alltel's billing execs won't need to hold a candle-
- lighting vigil preceding the rollout of its cdma2000 network, which is scheduled to launch in New Orleans and
Baton Rouge, LA, during the second half of this year.

Alltel already has dealt with usage-collection issues in packet-- based networks.

"We have these issues in our wireline business because we have packet networks on the wireline side," Lyons
said. "A lot of these issues are going to be new to the wireless business, but they're not without precedent in the
telecom industry."

Even on the wireless side of its business, Alltel has faced some of the complexities of extracting usage information from IP networks. The company operates CDPD networks in Phoenix, Cleveland and Tampa, FL.

"CDPD gives us a lot of insight into some of the practical pitfalls of managing and billing for a wireless IP-based network," Lyons said. "I'm not sure that it provides any level of evolution into 3G. But it provides us with a whole lot of expertise and background information."

One big lesson Alltel learned from its CDPD experience is that keeping track of IP-services usage depends on the ability to manage and assign IP numbers and use them as subscriber identifiers.

"We've all built our thought processes and our billing systems to be based on the phone number being the unique network identifier of a customer," Lyons said. "Particularly if you do revenue reporting for markets or regions based on phone numbers, you can rely on NPAs (numbering plan areas) and NXXs (exchanges or prefixes) to give you a geographic association between the phone numbers and your markets. IP numbers don't have that type of logic, unless you can assign them internally that way. And if you have dynamically assigned IP numbers, that's even messier because the IP address changes every session. So you have to have other ways to identify the customer."

The fundamental difference between IP and traditional telecom networks creates an added layer of complexity. Circuit-switched networks are centralized. A subscriber's calls travel through a switch, and his usage can be monitored through that switch. But in the decentralized IP environment, information about one call travels along multiple routes such as through a telecom switch, a WAP gateway and an application server.

Lyons mused about the possible complications of usage monitoring and billing as data services become more sophisticated and carriers' relationships with content and service providers become more intricate. He conjured the image of a subscriber roaming on Alltel's packet network. Distracted by a coffee craving, the subscriber uses a location-based service to locate the nearest Starbucks on a portable device, then accesses the coffee vendor's Web site and orders online so that his drink will be ready when he arrives at the store.

In Lyons's scenario, Starbucks has agreed to pay for the call whenever a customer orders coffee over Alltel's network. Such an arrangement would complicate the billing process, because Alltel would have to deduct the transaction for the subscriber's bill and add it to Starbucks' tab.

"That's a kind of out-there sce

Figure 2.

Figure 3.

nario," Lyons admitted. "But that's the type of thing that will happen, settlement with advertisers, settlement with content providers. The complexity is going to be preparing the infrastructure today for the things that might happen tomorrow."

To prepare for the applications of tomorrow, Alltel is trying to create a billing enterprise that is adaptable and operates on open architectures.

"You've got to have an infrastructure that's adaptive and flexible, because you may not get six to 12 months of lead time to develop things or issue requests for proposals," Lyons said. Vendors can help carriers by creating standards-based rather than proprietary architectures for their products and by considering carriers' billing and back-office needs, Lyons said.

Studying the Course

Anita Tsui, SmarTone spokesperson, said that vendors need to create standards that enable different kinds of routers and servers to communicate, as well as those that comply with existing data formats such as the TAP3 and Ciber roaming settlement formats.

SmarTone plans to launch its 3G network in 2002, if it is awarded a 3G license. The planning and preparation for IP usage data collection will take at least six months, Tsui said. But ultimately, the preparation time requirement depends on the complexity of the services the company decides to offer.

According to Tsui, the biggest challenge probably will be collecting roaming data.

"The mechanism and standards for data collection from roaming partners are still not yet determined," she said. Unresolved issues relative to roaming include whether carriers will charge each other based on time, volume, flat rates or using some other method and how data from various IP sources will be aggregated and analyzed.

Preparing for the Transition

Unfortunately, there is more than one answer to the question of how to collect usage information from IP networks. (See Figures 2 on page 32 and Figure 3 on page 34.)

"There are a variety of players in the IP-mediation environment and most of them have a different perspective on where you should measure usage," said Ace*Comm's Demers. "Should you use probes? Should you be collecting data from the network-- management platform? Should you be collecting data from the actual network elements?"

When a wireless network carries data from the Internet, a device known as a probe can be used to monitor the data stream and measure usage that way, Demers explained. Information also can be gathered from IP routers and network gateways.

Figure 4. Ace*Comm prefers to connect to all of the network gateways involved in a transaction to get an exact measurement of usage.

"But there are people that will connect to the network-management platform and gather statistics on usage rather than precise usage," Demers said. "Right now, the most widely used, secure and reliable way is to gather the actual data that the network elements generate. But in some cases, that doesn't give you the complete picture, so you also need information from proxy servers and other devices in the network that allow you to identify the user of the services."

Mark Fowlie, Amdocs vice president of product marketing, said that examples of network elements containing access information include:

* The WAP gateway
* Application servers, which hold application -usage information
* Commerce servers, which contain information about trade transactions
* AAA servers, which produce user-ID information. During the build-out of next-- generation networks, companies will have nationwide networks that will be a mixture of 1G, 2G, 2.5G and 3G technologies.

"This situation creates the requirement for convergence at the mediation and/or billing area," Fowlie said. "A convergent mediation layer collects information from all of the network technologies and routes it to the appropriate customer-care and billing system. A convergent customer care and billing system removes the need for a convergent mediation layer in that there is only one customer care and billing system for all services."

Amdocs works with mediation providers, which extract usage information from the switch, correlate it and pass it on to Amdocs for rating and mediation. In addition, the company is a member of the IPDR Organization, an association of vendors and a few carriers that has set out to define how to measure and exchange IP-related information between network elements, operation-support systems and business-support systems.

Hewlett-Packard also belongs to the IPDR Organization and has been studying the mediation needs created by merging wireless and the Internet for the past year and a half. The company recently released a version of its Internet mediation software that can extract information from Ericsson, Motorola and Nokia network equipment, as well as other wireless network elements.

"The IPDR Organization's basic plan and function is to make sure that we can continue to measure service for consumers or intercarrier," said Tom Russotto, Ace*Comm CTO. Russotto also serves as chairman of the IPDR Organization Interoperability Pavilion.

"We think it's going to be very important to set some standards that essentially the whole world can use to eliminate some of the problems that we have in the legacy world with so many different formats of information," Russotto said. "The effort within the IPDR Organization is a really good one for industry. But it would be helpful to have more carriers in there telling us about the things they're thinking about the future - the services they want to offer, the kinds of billing plans, the kinds of problems they anticipate with fraud, for instance, or network management or quality of service."

In October, the IPDR released Version 2 of its network-data management-usage standard. Version 2.5 of the standard, released in February, defines data-- exchange elements for a variety of services. THIS IS THE FULL-TEXT.

Compuware's Production Readiness Offering Provides Companies With Powerful
   E-commerce Performance Solutions

New QACenter Releases Offer Huge Advances in E-commerce Testing   FARMINGTON HILLS, Mich., Oct. 26 /PRNewswire/ -- Compuware Corporation (Nasdaq: CPWR) today announced significant upgrades to QACenter, the company's product family for e-commerce and client/ server testing. When teamed with Compuware's EcoSYSTEMS products, QACenter enables organizations to build reliable and scalable e-commerce applications. The upgrades to three core QACenter products, QARun, for functional and regression testing, QALoad, for performance, load and capacity testing and QADirector, for test planning and management, continue to advance Compuware's offerings for companies looking for comprehensive, cross-platform e-commerce solutions.

Compuware's Production Readiness

QALoad, coupled with the Compuware EcoSYSTEMS application service management offerings, provide organizations with a strategic, competitive advantage for e-commerce success. These products offer the industry's only integrated Production Readiness solution that enables scalability testing for high-volume sites. IT organizations that employ Compuware's Production Readiness solution can feel secure in knowing exactly how their e-commerce systems will perform after they go live.

"With recent, highly publicized failures of high-profile web sites, companies are learning firsthand that downtime to an organization's e-commerce site can be devastating," said Doug Turner, General Manager, Compuware QACenter. "Poor performing or unavailable sites can translate into a huge hit to a company's stock price, and, just as importantly, to a company's customer base, which is only a click away from the competition."

Load Testing and Production Readiness

QALoad (now shipping) can test a web application by simulating an unlimited number of users, allowing IT organizations to perform realistic tests on high-transaction and highly accessed web sites to determine how well the system can handle high levels of traffic. In testing external sites, Extranets and Intranets, QALoad measures user response times by simulating tens of thousands of users performing real actions, such as purchasing transactions, on the web site. This capability allows companies to determine how well their systems will perform during peak periods of use -- the Christmas buying season for example -- prior to the system being deployed in production. The features in this release continue to make it easier to analyze performance data and make sound business decisions.

EcoSYSTEMS and Production Readiness

With the ability to test thousands of users simultaneously accessing a web site, IT organizations, in order to gain a full understanding of system performance, must clearly understand what is also happening on servers and the network. The Compuware EcoSYSTEMS product suite manages, monitors and reports on application service levels, providing the critical ingredient to successfully implementing e-commerce applications. While using QALoad to determine user response times, IT organizations can use EcoSYSTEMS to gather resource utilization data that correlates with response times to diagnose potential problems before they occur. This information is presented in the form of easy-to-read graphs and reports, which provide realistic indications of system performance prior to deployment.

Testing for the Web

Compuware also announced that in the new release of QARun, its product for automated functional, regression and acceptance testing, all major web environments are now supported, including Java, DHTML, XML, ASP and Oracle NCA v11. The new version also supports cross-browser compatibility between Netscape Communicator and Microsoft Internet Explorer making them interchangeable throughout the testing process. Also now available as a standalone option is WebCheck, which tests for over 50 items that may affect the integrity of the web site, such as broken URLs and orphaned pages.

"It is crucial that companies implement the best tools and processes to understand how their critical e-commerce systems will perform prior to their deployment," said Turner. "There is too much evidence of high-profile sites not meeting customer demands, either by not performing or not being available. In the fast world of the web, this can spell disaster, not just in customer satisfaction but in overall company valuation as well."

QACenter Products in Use at Federal Express

QACenter products have been well received for e-commerce and Internet testing by some of the leading companies in the world; one such company is Federal Express Corporation (FedEx).

"As FedEx increases the number of Internet-based applications that will be distributed across multiple platforms, it becomes critical that we rigorously test them for reliability and scalability," said Christopher T. Hjelm, senior vice president and CIO of FedEx.

Among the systems that required automated testing at FedEx were those that tied handheld scanning devices and mobile radio systems to standard office environments, including server and standalone PCs.

"Our automated testing processes are designed to ensure applications function reliably before they reach our customers. Testing for scalability and peak loads has been very challenging, but these new tools are making testing even the most challenging of items a reality," continued Hjelm.

FedEx is also testing its international custom clearance systems. These applications are critical to ensuring that the company can provide the most reliable and effective level of service to its customers.

"The speed of the Internet along with increased customer expectations means that it is critical that our systems run faultlessly. As a leader in e-commerce, FedEx must continue to deliver the highest quality applications and systems possible," added Hjelm.

QACenter

QACenter is a family of automated testing products and services for web-based, client/ server , mid-range hosted, ERP and mainframe applications. QALoad measures end-to-end response times by simulating thousands of users without requiring additional hardware or end-users. Coupled with Compuware EcoSYSTEMS, customers have a complete view of how their applications will perform in production before they are deployed. QARun features automated testing functions required by companies developing, shipping or maintaining business-critical web, ERP or enterprise applications. The Compuware mainframe automated testing products, QAHiperstation and QABatch, have been standards in IS organizations for the past decade. Other products in the family include QADirector, for test process management and TrackRecord for enterprise-wide defect tracking. QASolutions offers customers a comprehensive testing solution, including industry leading products and professional services.

Compuware Corporation

Compuware productivity solutions help 14,000 of the world's largest corporations more efficiently maintain and enhance their most critical business applications. Providing immediate and measurable return on information technology investments, Compuware products and services improve quality, lower costs and increase the speed at which systems can be developed, implemented and supported. Compuware employs approximately 15,000 information technology professionals worldwide. With trailing 12-month revenues of more than $1.9 billion, Compuware is a world leader in the practical implementation of enterprise and e-commerce solutions. For more information about Compuware, please contact the corporate offices at 800-521- 9353. You may also visit Compuware on the World Wide Web at www.compuware.com

For sales or marketing information:

Compuware Corporation, 31440 Northwestern Highway, Farmington Hills, MI 48334, Tel: 800-521-9353, www.compuware.com

Compuware, QACenter, QARun, QALoad, EcoSYSTEMS, UNIFACE, QAHiperstation, QABatch, QADirector, TrackRecord and QASolutions are trademarks or registered trademarks of Compuware Corporation. All other product and company names are trademarks or registered trademarks of their respective owners.

/CONTACT: Steve Reilly, steve_reilly@compuware.com, or Fred Diamond, fred_diamond@compuware.com, of Compuware Corporation, 248-737-7300/ 10:52 EDT

Copyright 1999 PR Newswire. Source: World Reporter (Trade Mark).

COMPANY NAMES: Compuware Corp

DESCRIPTORS: Company News

SIC CODES/DESCRIPTIONS: 7375 (Information Retrieval Services); 5961
 (Catalog & Mail Order Houses)

NAICS CODES/DESCRIPTIONS: 514191 (On-Line Information Services); 45411
 (Electronic Shopping & Mail-Order Houses)

xSPs Can Improve Service, Time-to-Market, Profitability, and Reliability

SANTA CRUZ, Calif., and ISLANDIA, N.Y., April 16 /PRNewswire/ -- Tarantella, Inc., a wholly owned subsidiary of The Santa Cruz Operation, Inc. (Nasdaq: SCOC), and iCan SP, Inc., a subsidiary of Computer Associates International, Inc. (NYSE: CA), specializing in business and operations support software for xSPs, today announced a joint marketing and sales agreement, through which the two companies will leverage each other's technologies to provide complete solutions for hosted-service and infrastructure providers.

Tarantella, a major force in enterprise computing, hosted solutions and eCommerce, provides state-of-the-art software that delivers applications through a Web browser. iCan SP offers the industry's only comprehensive, end-to-end business operations solution for the hosted-services environment. Together, Tarantella Enterprise 3 and the iCan Provider Suite enable large enterprises to provide applications via the Web. Using these paired offerings, both enterprises and xSPs can provision applications, manage service levels and support a wide range of hosted services.

"The market has clearly defined the need for service providers -- and that includes many corporate IT departments -- to focus on core business competencies," said iCan CEO Nancy. Li. "Combining the strength of Tarantella Enterprise 3 and the iCan Provider Suite underscores our commitment to support that focus. Tarantella and iCan make xSPs more pervasive, more profitable, and more reliable, while helping to reduce their time to market with new service offerings."

"The chronic, persistent IT shortage has made it difficult for businesses to operate at today's competitive pace," said Dennis Adams, vice president of world-wide marketing for Tarantella, Inc. "Smart companies are turning to service provider models, using Web-client technologies to help them extend their reach to employees, customers and suppliers around the world. Together, iCan SP and Tarantella will offer xSPs -- including self-servicing enterprises -- the means to create reliable, robust, end-to-end solutions without disruption or major infrastructure overhauls."

Tarantella Enterprise 3 software Web-enables and supports the central management of applications running on Windows, UNIX, Linux, AS/400 and mainframe computers without rewrites, so that they can be instantly deployed to authorized users anywhere, anytime. Because it is compatible with Web-based, as well as traditional and client/ server applications, Tarantella is a key component to the adoption of the Web as the ultimate user and administration interface and integration environment.

The iCan Provider Suite lets hosted-service providers provision, meter, manage, bill and brand their services in a highly automated and flexible manner that meets their customers' varied requirements. Components of the iCan Provider Suite include: -- iCan Meter -- lets xSPs collect usage and performance data across all domains and generate activity reports. -- iCan Assure -- lets xSPs predefine service packages to meet a wide range of customer requirements. -- iCan Provision -- allows xSP's customers to select and order the service package that best meets their needs. -- iCan Bill -- provides real-time usage and event-based billing. -- iCan View -- lets xSPs and their customers view, access and administer their services through a customizable portal.

Using Tarantella Enterprise 3 and the iCan Provider Suite gives hosted-service providers the ability to deliver, support and centrally manage any application via the Web, along with a complete range of customer service, administrative and billing services. xSPs can obtain all the necessary software for this complete solution through a single source-either Tarantella, iCan SP or any of either company's authorized channel partners.

"Suppliers and customers can only recognize the merits of an xSP offering when the service is supported by a solid delivery and management infrastructure," said Amy Mizoras, Senior Analyst at IDC. "The combined Tarantella and iCan SP solution can help service providers or enterprises enable, manage, and support the Web-delivery of their applications."

About Tarantella, Inc.

Tarantella, Inc., a wholly owned subsidiary of The Santa Cruz Operation, Inc., promotes Web-enabling software technologies that connect clients,   server -based applications, and networks. The Tarantella product line includes Tarantella Enterprise 3 Web-enabling software for large companies and organizations; Tarantella Enterprise 3, ASP Edition, for Application Service Providers; and Tarantella Express for workgroup and

departmental environments. Tarantella products provide access to Microsoft Windows, mainframe, AS/400, Linux and UNIX applications. For more information, go to http://www.tarantella.com.

About iCan SP

iCan SP, Inc., a wholly owned subsidiary of Computer Associates International, Inc. (CA), provides business and operations support software for the hosted-services industry. iCan's software solutions enable xSPs and others to enhance their service offerings and further capitalize on today's rapidly growing market for hosted services. For more information visit http://www.icansp.com.

About Computer Associates

Computer Associates International, Inc. (NYSE: CA) delivers The Software That Manages eBusiness. CA's world-class solutions address all aspects of eBusiness process management, information management, and infrastructure management in six focus areas: enterprise management, security, storage, eBusiness transformation and integration, portal and knowledge management, and predictive analysis and visualization. Founded in 1976, CA serves organizations in more than 100 countries, including 99 percent of the Fortune 500 companies. For more information, please visit http://ca.com.

The Santa Cruz Operation, SCO, Tarantella, Tarantella Enterprise 3, Tarantella Enterprise 3, ASP Edition, Tarantella Express, and the Tarantella logo are trademarks or registered trademarks of The Santa Cruz Operation, Inc. in the USA and other countries. UNIX is a trademark of The Open Group in the United States and other countries. Windows is a registered trademark of Microsoft Corporation in the US and other countries. Linux is a trademark of Linus Torvalds. AS/400 is a registered trademark of International Business Machines Corporation in the USA and other countries. All other brand and product names are or may be trademarks of, and are used to identify products or services of their respective owners.

/CONTACT: Elliot Kass of Tarantella, Inc., 631-904-3045, bettek@tarantella.com; Bette Kun of iCan SP, Inc., 831-427-7397, elliot.kass@icansp.com/ 09:30 EDT

Copyright 2001 PR Newswire. Source: World Reporter (Trade Mark).
COMPANY NAMES: Santa Cruz Operation Inc
DESCRIPTORS: Joint Ventures; Strategy; Company News; Marketing
COUNTRY NAMES/CODES: United States of America (US)
REGIONS: Americas; North America; Pacific Rim
PROVINCE/STATE: California

TEXT:

Companies have monitored employees for security and work measurement purposes for years. However, the scope of monitoring activities has expanded in recent years with development of electronic tools, and the number of companies that monitor employee activities has also increased. According to a June 22, 2000, report in USA Today, about 74 percent of companies currently conduct some form of electronic monitoring of employee activities whereas in 1977 only 35 percent of companies were engaged in electronic monitoring. (1) Given the growth in electronic monitoring activities, CPAs increasingly are expected to respond to their client's questions with respect to both the tools available to monitor employee activity and the potential legal and social impacts of using those tools.

Activities Monitored

At many companies, access to the Internet has replaced the office water cooler as a social gathering place within the work environment, and managers are concerned about the potential loss of productivity and the security of proprietary information. Observing idle time around the water cooler is easy, but electronic activities are not so visible. Likewise, securing the company data was easier when physical removal from the premises was the only major threat.

In the past, most workplace monitoring activities required the presence of a physical monitoring device such as a video camera or a person. Electronic monitoring of e-mail, computer files, Web sites accessed, keystrokes, phone time and other computer -related activity does not require a physical presence and can be hidden completely from the monitored employee. The diversity of electronic monitoring of employees is captured in the following table from data gathered by the American Management Association's 2000 Monitoring and Surveillance Survey.

Monitoring Tools

Electronic monitoring tools fail into one of two categories: (1) those that monitor all employee computing activities or (2) those that monitor only Internet-related employee activities. Within the second category, tools are available that can monitor all Internet-related activities or only selected tasks such as e-mail. E-mail appears to be of particular interest to many organizations. Sales of e-mail monitoring tools are expected to reach $70 million this year and to double within the next few years. (3)

An example of software that monitors all computing activities is Investigator by WinWhatWhere Corporation. The program, installed on each user's computer , can log every Web site visited, documents and files opened, and time spent on each application . Because Investigator captures all key-strokes, it also can monitor deleted or unsent e-mail messages and documents. Investigator's installation is not apparent to the user. Prices start at $99 per user with downward adjustments based on volume.   An example of software that monitors only Internet usage is NetSpective by Telemate.Net Software, Inc. This program is installed on an organization's proxy server or firewall and monitors all employee Internet activities, including e-mail, Web site visits and downloads. NetSpective can block access to nonproductive Web sites or to high band-width downloads (such as audio or video files). The program can report on Internet e-mail traffic and band-width consumption by users, groups, or peak times. The software's drill-down reporting capability permits network managers to monitor virtually any usage down to the user level. Prices for NetSpective start at $995 per proxy server for simple Internet usage reporting and can range upward to $15,000 per proxy server if a business wishes to implement all features of the system including active blocking of access to specific Web sites or other Internet activities.

Legal Issues

Government versus Private Employee Rights

CPAs who have government agencies as clients should be aware of the fact that monitoring of employees in such agencies normally is prohibited by the Fourth Amendment to the U.S. Constitution, which bars unreasonable searches and seizures. In addition, several states have specific constitutional provisions that recognize state employees' rights to privacy. (4)

Unlike public employees, private employees are not afforded a constitutional right to privacy in the workplace. In general, if employees are informed of the surveillance possibility, and the activity is not prohibited specifically by contract or law, surveillance is permitted. (5) Sometimes, employers have won court decisions in their favor when sued for monitoring activities even after providing assurances of privacy. (6)

Current Litigation and Proposed Legislation

Some employees have brought civil damage suits against their employers under the Electronic Communications Privacy Act (ECPA) of 1986. With respect to electronic communications, this act prohibits· unauthorized interception and unauthorized retrieval from storage media, such as hard disks. The act provides an exception for employers; specifically, if one of the parties to the communication has consented, interception is allowed. Whether the ECPA applies to communications over a business' private network is unclear at present, even more so when a business' private network utilizes an external network such as the Internet. (7)

Legislation currently before the Congress will, if adopted, prohibit companies from secretly monitoring their employees' e-mail and Internet usage. A bill before the House, known as the Notice of Electronic Monitoring Act, would not prohibit employee monitoring but would (1) require notification to employees of the firm's monitoring practices on an annual basis or whenever policies are changed, (2) require specific disclosure as to the frequency of monitoring, where the information is stored and how it will be used, and (3) limit civil damages to $20,000. Essentially identical legislation is pending in the Senate. (8) Similar legislation has been proposed in prior congressional sessions, and it seems likely that some legislation will be passed in the relatively near future.

International Legal Ramifications

Since many clients have international operations that utilize Internet-based systems, CPAs should be aware that other countries such as Canada and England have different legal frameworks covering electronic monitoring of employees. A measure taking effect in October 2000 in England makes it illegal to monitor employees electronically without consent--even for purposes such as staff training, marketing and market research. (9) The Criminal Code of Canada prohibits the interception of private communications in that country. (10)

In general, employers can protect their legal right to monitor employee e-mail and other Internet-related activities by properly notifying employees of their monitoring policies and obtaining employee consent. The American Management Association recommends the following to its member companies:

Policies and practices in electronic monitoring and surveillance should be promulgated and posted so that employees are aware that their actions and communications are subject to recording and review. (11)   In its 2000 survey, the American Management Association found that over 85 percent of reporting firms inform employees of their electronic monitoring policies. (12)

Monitoring and Employee Morale Issues

Beyond the legal issues, CPAs and their clients must be cognizant of the possible impact of electronic monitoring on employee trust and morale. Because broad-based monitoring of key strokes or Internet-related activities is a relatively recent phenomenon, little specific empirical work centered on such practices exists. However, electronic monitoring of employee activities in call-centers has been widely studied and provides some pertinent insights.

Privacy advocates have written extensively on the negative aspects of employee monitoring. However, empirical research examining call-centers does not seem to support the hypothesis that employee monitoring necessarily generates negative employee responses. A comparison of employee attitudes in five different companies in five different industries suggests that whether employees respond positively or negatively to monitoring depends on how the monitoring is implemented and how the collected data is used. (13)

Whether monitoring is for purposes of reviewing employee performance, protecting company secrets, or enforcing workplace rules, research results suggest that employees will be more satisfied if they believe that the system is procedurally fair. A process is considered procedurally fair when it includes input from all affected parties, is applied consistently, suppresses bias, is as accurate as possible, provides a mechanism for correcting errors and is ethical. (14) Perceived lack of procedural fairness in electronic monitoring can lead to undesirable negative employee reactions such as withdrawal, sabotage, resignation or some other form of diminished organizational citizenship. (15)

An electronic employee-monitoring system is more likely to find acceptance with employees if, in addition to being procedurally just, the use of the collected data is thought to be distributively just. A system is considered distributively just if employees perceive the outputs of the system as related fairly to personal outcomes, such as individual pay or promotion. Thus, if employees perceive that pay or other rewards are distributed in a way that is consistent with the data reported by the monitoring system, the system will be thought of as distributively just. Perceived lack of distributive justice in an electronic monitoring system has been shown to be associated with lower job satisfaction in non-government organizations. (16)

Recommendations

To Monitor or Not

Unless the employer is a government agency, a fundamental right to monitor employee activity exists at the present time. As clients seek advice on the implementation of employee monitoring tools, the first question that must be addressed is the business purpose of the monitoring. Electronic monitoring is costly, and the benefits should exceed the costs. In addition to the software costs cited earlier, additional costs include the time to review and use the collected data and the high cost of employee dissatisfaction if the electronic monitoring system is not properly designed and implemented.

Proponents of monitoring argue that the economic benefits include reduction of nonproductive use of company assets and the safety of proprietary information. Unfortunately, clever employees who wish to steal proprietary information are often knowledgeable enough to elude any monitoring system in place. Further, if the productivity of an employee meets or exceeds the expectations of the employer, little reason to monitor his or her activities exists. In fact, opponents to monitoring argue that a productive employee's personal use of the firm's electronic applications is a good employer accommodation that allows such employees to be the productive people that they are. Monitoring opponents also maintain that employees performing at substandard levels are unlikely to change just because a monitoring system is put into place.

Compliance with legal requirements is another reason to implement electronic monitoring. In regulated industries, taping telemarketing activities may provide both the company and its customers some degree of legal protection by providing accurate records of activities. Electronic recording and storage of activities might be considered part of the company's due diligence in keeping adequate records and files of its activities.

Arguments are sometimes made that electronic monitoring is one way that an organization can guard against an employee's unwitting exposure to offensive graphic material on a colleague's computer screen or one employee harassing another through e-mail or other electronic communication. Employers do not have a duty to discover harassment. They do have a clear duty to take action to prevent the recurrence of such activity once discovered. However, that would involve monitoring a specific individual's activities rather than an entire work-force, clearly a much less costly proposition. (18)

Implementation Guidelines

If a client is convinced that sound business reasons exist to implement electronic monitoring, then CPAs must be prepared to offer sound implementation advice. The following guidelines appear to provide a reasonable basis for monitoring activities in order to avoid potential problems.

* Establish a reasonable and clear policy with respect to Internet activities. A general policy stating that illegal and non-work-related tasks done over the Internet are prohibited should be sufficient. Policies that attempt to list every non-permitted activity typically fail because of overlooked or new activities. Further, detailed policies create the illusion of acceptance for any activity excluded from the list.

* Create a privacy policy that clearly informs employees about the monitoring activities that are in place and the use of the gathered data. Then, follow the stated policy. Changes in either monitoring efforts or usage of gathered data should be announced publicly prior to implementation. Care should be taken when developing privacy policies so that employees understand the fairness of both the policy and the use of gathered data. Stated policies that are consistently followed are the best defense against employee lawsuits.

Conclusion

* Provide security training for everyone with access to the Internet. Employees need to be aware of the potential harm that can occur--either to themselves as individuals or to the organization--given the insecure nature of Internet transactions. Employees must realize that privacy and security of e-mail, Web sessions and other Internet-based activities do not exist and that any information passed between computers during such sessions is open to others both inside and outside the firm.

While electronic monitoring of employee activity is widespread and growing, empirical work that provides insight into the costs and benefits of such monitoring is not yet available. Results of monitoring activity can be neutral, positive or negative to an organization's productivity and employee morale depending on implementation. Managers must explore the costs and benefits of electronic employee monitoring technology to see if the benefits exceed the costs. When a decision is made to implement tools that electronically monitor employee activities, managers should develop policies for implementation that are procedurally and distributively just and emphasize performance rather than control. Without adequate supporting policies, achieving the expected benefits may be difficult.

Mark F. Asman, Ph.D., CPA, CDP, Ernst & Young, is professor emeritus of accounting and MIS at Bowling Green State University in Bowling Green, Ohio 43403.

Patricia A. Essex, Ph.D., CPA, is an associate professor of accounting and MIS at Bowling Green State University in Bowling Green, Ohio 43403.

Endnotes

(1.) USA Today, June 22, 2000, p. B1.

(2.) Greenberg, Eric Rolfe, Carol Canzoneri, and Joe Annamma, "A 2000 Survey, Workplace Testing; Monitoring and Surveillance," American Management Association, p. 1.

(3.) Informationweek, February 21, 1000, pp. 142-146.

(4.) Overly, Michael R., E-Policy, American Management Association, 1999, pp. 23-30.

(5.) Hertenstein, Edward, Dispute Resolution Journal, Vol. 52, No. 4, Fall, 1997, pp. 36-44.

(6.) See the California case of Shoard v. Epson America, Inc.

(7.) Overly, Michael R., Ibid.

(8.) Thibodeau, Patrick, Computerworld, September 11, 2000, pp. 1; 95.

(9.) Eaglesham, Jean, Financial Times, London Edition, August 3, 2000.

(10.) Gahtan, Alan, Canadian Business and Current Affairs, March 1997, p. 2.

(11.) Greenberg, et. al. Ibid.

(12.) Ibid.

(13.) George, Joey F., " Computer -Based Monitoring: Common Perceptions and Empirical Results," MIS Quarterly, December 1966.

(14.) Leventhal, G.S., "What Should be Done with Equity Theory? New Approaches to the Study of Fairness in Social Relationships." In K. Gergen, M. Greenberg, & R. Willis (Eds.), Social Exchange: Advances in Theory and Research, pp. 27-55. New York: Plenum, 1980.

(15.) Kidwell, Jr., Roland E. and Nathan Bennett, "Employee Reactions to Electronic Control Systems, The Role of Procedural Fairness," Group & Organizational Management, Vol. 19, No. 2, June 1994, pp. 203-218.

(16.) Ibid.

(17.) Hodson, Thomas J., Fred Englander, and Valerie Englander, "Ethical, Legal, and Economic Aspects of Employee Monitoring of Employee Electronic Mail," Journal of Business Ethics, Vol. 19, No. 1, March 1999.

Diversity of Monitoring Activities (2)

Electronic Activity Monitored	Percent of Reporting Firms Monitoring
Monitor Internet connections	54.1%
Telephone use (time spent, numbers called)	44.0%
Store and review e-mail messages	38.1%
Store and review computer files	30.8%
Computer use (time logged on, keystroke counts, etc.)	19.4%
Record and review telephone conversations	11.5%
Store and review voice mail messages	6.8%

Source: American Management Association

FILE SEGMENT: MC File 75

COMPANY NAMES: WinWhatWhere Corp.--Products; Telemate.Net Software Inc.-- .Products

INDUSTRY CODES/NAMES: BANK Banking, Finance and Accounting; BUSN Any type of business; REG Business, Regional

DESCRIPTORS: United States. Congress--Laws, regulations, etc.; American Management Association--Surveys; Electronic employee monitoring--Laws, regulations, etc.; Computer software industry--Products; Online services--Laws, regulations, etc

GEOGRAPHIC CODES/NAMES: 1USA United States

PRODUCT/INDUSTRY NAMES: 7372000 (Computer Software); 3662700 (Electronic Systems & Equip NEC); 4811520 (Online Services); 9125600 (Employment Standards Admin

SIC CODES: 7372 Prepackaged software; 4822 Telegraph & other communications

NAICS CODES: 51121 Software Publishers; 33599 All Other Electrical Equipment and Component Manufacturing; 514191 On-Line Information Services; 92615 Regulation, Licensing, and Inspection of Miscellaneous Commercial Sectors

-- Companies Form Strategic Partnership to Combine Comprehensive IP Mediation with Internet Billing and Customer Care System

SANTA CLARA and CUPERTINO, Calif. -- XACCT Technologies, Inc., which makes the XACCTusage metering and mediation solution for IP networks, and Portal Software, Inc., a leading provider of software for Internet and emerging next-generation communications services, today announced that they have entered into a strategic partnership. Under the terms of the agreement, XACCT will integrate XACCTusage with Portal's Infranet customer management and billing software.

The basic flat-rate model used today for IP billing does not work well for emerging value-added services such as IP telephony, IP fax, and streaming audio/video. A growing number of Network Service Providers (NSPs) now realise that they must bill such services based on a variety of parameters, not just on "time-on-line". Together, XACCTusage and Infranet will enable NSPs to generate accurate, usage-based bills based on detailed information about applications, Quality of Service (QoS), time of day, and other parameters.

"We are excited to partner with XACCT," said Jill Kyte, senior director, strategic alliances, at Portal. "XACCT's technology for collecting data and performing mediation in real time meshes perfectly with Portal's Real-Time/No-Limits philosophy. This combination will provide a powerful solution for those emerging companies that want the flexibility to charge users for on-line services based on any aspect of service delivery."

Complementary Solutions

Infranet is the most flexible, scalable, real-time billing solution available in the market, enabling service providers to rapidly deploy innovative services with sophisticated pricing models.

XACCTusage provides a single mediation interface between the customer care and billing application and the IP infrastructure. It collects and aggregates accurate, detailed usage data from multiple network elements and application servers to create XACCT detail records (XDR), the IP equivalent of the Call Detail Records (CDRs) generated by telephone switches. The XDRs are used by Portal's Infranet to generate transaction-based bills.

"The Portal and XACCT products are highly synergistic. Together, they empower the service providers to offer differentiated value-added services, quickly and profitably," said Anil Uberoi, vice president of marketing at XACCT. "With XACCTusage and Portal's Infranet, customers can introduce new, innovative services and adjust pricing plans that meet changing market needs.

End-to-End, Real-Time Capabilities

Portal's Infranet software is designed specifically for next-generation communications services and is the only customer management and billing solution available with true, end-to-end, real-time capabilities. XACCTusage complements Infranet with real-time service metering and usage data feed. These capabilities enable IP service providers to rapidly introduce innovative, value-added services and flexible pricing plans that they can adjust within minutes based on market or competitive demands. Infranet also reduces customer service costs by enabling "self-help" customer support features that provide instant access to service or billing information via the Web.

Multi-source, Multi-layer Architecture

XACCTusage is a flexible, scalable solution that lets service providers precisely define the IP session information they wish to capture. XACCT's multi-source, multi-layered approach to data collection enables the software to collect network usage data from multiple network elements, including routers, switches, firewalls and a variety of application servers, spanning all layers of the network - from the physical layer to the application layer. Real-time, policy-based filtering, aggregation and enhancement of the transaction data produces accurate, detailed records for customer bills. Additionally, this information enables service providers to accurately assess the costs associated with the services they offer, based on actual network resource consumption. The architecture makes XACCTusage an ideal solution for multi-vendor, heterogeneous networks.

Automated Service Provisioning

NSPs can also automate end-to-end service provisioning by using XACCTusage to mediate between Portal's Infranet and the various network elements for service activation, authentication and authorisation. This allows service providers to minimise their service activation lead-times and start capturing revenue immediately.

About Portal Software, Inc.

Portal Software, Inc., is the link between services, customers and revenues for Internet and next-generation communications services. Portal's real-time customer management and billing software enables Internet and next-generation communications services to rapidly develop, price and provision new services and effectively manage customer usage and billing. The combination of Portal's real-time technology and flexibility allows Internet service and communications companies to generate more revenue and be more competitive by enabling them to bring new services to market quicker than ever before and by establishing innovative ways of supporting and reacting to customer's needs. Target markets include Internet access businesses; next-generation IP-based services such as Internet telephony and virtual private networks (VPNs); and web and application hosting, e-mail and unified messaging, online content services and other emerging IP based consumer and business services.

Portal's customers include leading Internet businesses worldwide such as US WEST, Microsoft, UUNET Technologies, BellSouth, Grolier Online, Palm Computing, France Telecom, OzEmail, Juno, USinternetworking and Verisign. Headquartered in Cupertino, California, Portal has offices throughout the U.S., as well as Hong Kong, Sydney and London. Information about Portal and its products can be found at http://www.portal.com.

About XACCT Technologies

XACCT Technologies, Inc., was founded in May 1997 and is headquartered in Santa Clara, Calif. The company has established itself as the market leader in the emerging IP mediation market. XACCT develops a new class of intelligent software solutions that enable Service Providers and enterprises to accurately account and bill for metered services and applications. Data Communications magazine recognised XACCT as one of the "Top 25 Hot Startups of 1998" and named XACCTusage as one of the "Hot Products of 1999." XACCT markets its software directly and through network systems integrators to Service Providers and Fortune 1000 companies. A privately held corporation, XACCT is funded by venture capital investors. More.information is available at http://www.xacct.com.

XACCTusage and XDR are trademarks of XACCT Technologies, Inc. Portal and Infranet are U.S. registered trademarks, and Portal Software, the Portal logo and the Real Time-No Limits tagline are trademarks of Portal Software, Inc.

CONTACT: Anil Uberoi, VP Marketing, XACCT Technologies, Inc. Tel: +1 408 654 9900 x 111 Fax: +1 408 654 9904 e-mail: anil@xacct.com WWW: http://www.xacct.com Lynne Rocha, Portal Software, Inc. Tel: +1 408 343 4397 e-mail: Lrocha@portal.com Charlotte Gutman, Communications for Genial Products SA - Brussels Tel: +32 2 375 21 00 Fax: +32 2 375 91 62 e-mail: cgp@cgp.be WWW: http://www.cgp.be Sharon Frais, Public Relations, CGP SA Tel: +32 2 375 21 00 Fax: +32 2 375 91 62 e-mail: sharon@cgp.be WWW: http://www.cgp.be

DESCRIPTORS: Facilities & Equipment; Company News; New Products & Services; Marketing; Contracts or New Orders
COUNTRY NAMES/CODES: United States of America (US)
REGIONS: Americas; North America; Pacific Rim
SIC CODES/DESCRIPTIONS: 7372 (Prepackaged Software)